Orbits on n-tuples

Ross Applegate and Peter J. Cameron*
School of Mathematical Sciences
Queen Mary, University of London
Mile End Road, London E1 4NS, UK

Abstract

A transitive (infinite) permutation group which has m orbits on ordered pairs of distinct points has at least m^{n-1} orbits on ordered n-tuples. This is best possible, and groups attaining the bound can be characterised.

1 Introduction

A permutation group G on an (infinite) set Ω is *oligomorphic* if the number of orbits of G on ordered n-tuples of distinct points of Ω is finite for all n. We refer to [1] for basic terminology and facts about permutation groups, especially oligomorphic permutation groups.

Let $F_n(G)$ (or just F_n, if the group G is clear from the context) be the number of orbits of G on the set of ordered n-tuples of distinct elements. It is easy to see that the sequence $F_n(G)$ is non-decreasing, since each orbit on such n-tuples consists of the initial segments of elements of at least one orbit on $(n+1)$-tuples of distinct elements. In particular, $F_n(G) = 1$ for all n if and only if G is *highly transitive*. This paper is a contribution to the question: how fast does the sequence (F_n) grow?

Of course it may not grow at all. If G is the symmetric group (or, indeed, if G is highly transitive), then $F_n = 1$ for all n. In other cases, the growth rate may be quite slow. For example, if G is the stabiliser of one point in the

*Corresponding author; email p.j.cameron@qmul.ac.uk

symmetric group, then $F_n = n+1$: there is one orbit of n-tuples with the fixed point in the ith position for $1 \le i \le n$, and one orbit not containing the fixed point.

At the other extreme, Merola [4] showed that, if G is primitive (that is, preserves no non-trivial equivalence relation on Ω) and not highly transitive, then

$$F_n(G) \geq \frac{c^n n!}{p(n)}$$

for some polynomial p, where c is an absolute constant; her proof shows that $c \geq 1.324$. There are known examples with $c = 2$. Results are also known about the number of orbits on unordered n-sets; see Macpherson [3].

We are concerned with the intermediate case, where G is assumed to be transitive but not necessarily primitive. Our result holds for all transitive but not 2-transitive groups G, and gives exponential growth for $F_n(G)$. Moreover, it is best possible.

Theorem 1 *Let G be an infinite transitive permutation group with $F_2(G) = m > 1$. Then $F_n(G) \geq m^{n-1}$ for all natural numbers n. Moreover, if $F_3(G) = m^2$ and $F_4(G) = m^3$, then G is imprimitive, with m infinite blocks of imprimitivity; the blocks are permuted regularly by G, and the stabiliser of a block acts k-transitively on it if $F_k(G) = m^{k-1}$.*

Remarks Let G be the wreath product of the cyclic group of order 2 and the infinite symmetric group. Then $F_n(G)$ is equal to the number of solutions of $g^2 = 1$ in the symmetric group S_n. In particular, $F_1(G) = 1$, $F_2(G) = 2$, $F_3(G) = 4$ and $F_4(G) = 10$. So the conditions of the theorem are best possible.

On the other hand, if G is the wreath product of a highly transitive group with a finite group of order s (acting regularly), then $F_n(G) = s^{n-1}$ for all $n \geq 1$.

2 Counting orbits

Let $F_1(x)$ and $F_2(x)$ be formal power series. We write $F_1(x) \succcurlyeq F_2(x)$ if the coefficients of F_1 are not less than those for F_2.

Lemma 2.1 *Let G be a transitive permutation group in which G_α has $r + s$ orbits on the remaining points, of which r are finite and s are infinite. Let*

$F_G(x) = \sum F_n(G)x^n/n!$. Moreover, let

$$\begin{aligned} f_r(x) &= 1 + \frac{1}{r+1}((1+x)^{r+1} - 1) = 1 + x + \frac{rx^2}{2!} + \frac{r(r-1)x^3}{3!} + \cdots, \\ g_s(x) &= 1 + \frac{1}{s}(\exp(sx) - 1) = 1 + x + \frac{sx^2}{2!} + \frac{s^2x^3}{3!} + \cdots . \end{aligned}$$

Then

(a) if $s = 0$, then $F_G(x) \succcurlyeq f_r(x)$;

(b) if $s \geq 1$, then $F_G(x) \succcurlyeq g_s(f_r(x) - 1)$.

Proof (a) Since G is transitive, we have

$$F_n(G) = F_{n-1}(G_\alpha) \geq r(r-1)\cdots(r-n+1).$$

(b) Again G is transitive, so $F_n(G) = F_{n-1}(G_\alpha)$. Moreover, the union of the finite G_α-orbits (including $\{\alpha\}$) is a block of imprimitivity for G.

Now we use a principle which occurs often in combinatorial enumeration, and is perhaps clearest in the context of species (Joyal [2]). Suppose that $\mathcal{F}$ and $\mathcal{G}$ are two species in which the exponential generating functions for labelled structures are $F(x)$ and $G(x)$ respectively. Then the exponential generating function for the species $\mathcal{G} \circ \mathcal{F}$ in which a structure consists of a set carrying a partition, with an $\mathcal{F}$-structure on each part and a $\mathcal{G}$-structure on the set of parts, is $G(F(x) - 1)$.

We apply this theorem with $\mathcal{F}$ the species of subsets of a block of imprimitivity, so that $F(x) \succcurlyeq f_r(x)$, and $\mathcal{G}$ a species defined as follows: given n points $x_1, \ldots, x_n$, the points different from x_1 are coloured with s colours, so that there are s^{n-1} labelled n-element structures for all n. Any orbit of G on n-tuples gives rise to a $\mathcal{G} \circ \mathcal{F}$-structure: the n-tuple is partitioned by the blocks of imprimitivity of its members, each part is a subset of a block, and the parts other than the first are coloured by the orbits of G_α containing the corresponding blocks, where α is the first point of the n-tuple.

So the exponential generating function for $(F_n(G))$ dominates the counting series for $\mathcal{G} \circ \mathcal{F}$, and the assertion is proved. □

Lemma 2.2 *Let G be an infinite transitive permutation group in which the stabiliser of a point has $r + s$ orbits, of which r are finite and s are infinite. Then* *(a)* $F_3(G) \geq (r+s)^2$, *with equality only if* $r = 0$ *or* $s = 1$.

(b) $F_4(G) \geq (r+s)^3$, *with equality only if* $r = 0$.

Proof Let $h(x) = g_s(f_r(x) - 1)$. We have

$$\begin{aligned} h(x) &= 1 + x + \frac{rx^2}{2} + \frac{r(r-1)x^3}{6} + \frac{r(r-1)(r-2)x^4}{24} + \cdots \\ &\quad + \frac{s}{2!}\left(x + \frac{rx^2}{2} + \frac{r(r-1)x^3}{6} + \cdots\right)^2 \\ &\quad + \frac{s^2}{3!}\left(x + \frac{rx^2}{2} + \cdots\right)^3 \\ &\quad + \frac{s^3}{4!}(x + \cdots)^4 + \cdots \end{aligned}$$

The coefficients of 1, x and $x^2/2!$ are 1, 1 and $r+s$. The coefficient of $x^3/3!$ is

$$r(r-1) + 3sr + s^2 = (r+s)^2 + (s-1)r;$$

this is at least $(r+s)^2$, with equality only if $r = 0$ or $s = 1$.

The coefficient of $x^4/4!$ is

$$r(r-1)(r-2) + 4r(r-1)s + 3r^2s + 6rs^2 + s^3 \geq (r+s)^3,$$

the difference between the two sides being $r^2(4s-3) + r(3s^2 - 4s + 2)$. This difference is positive if and only if $r > 0$.

Since $F_G(x) \succcurlyeq h(x)$, the lemma is proved. □

In the next section, we examine $h(x)$ further and show that the coefficient of $x^n/n!$ is at least $(r+s)^n$ for all n. This will complete the proof of the inequality in the theorem.

3 The exponential of a polynomial

Lemma 3.1 *Let* r *and* s *be positive integers. Let*

$$\begin{aligned} f_r(x) &= 1 + \frac{1}{r+1}((1+x)^{r+1} - 1) = 1 + x + \frac{rx^2}{2!} + \frac{r(r-1)x^3}{3!} + \cdots, \\ g_s(x) &= 1 + \frac{1}{s}(\exp(sx) - 1) = 1 + x + \frac{sx^2}{2!} + \frac{s^2x^3}{3!} + \cdots . \end{aligned}$$

and let

$$g_s(f_r(x)-1)=\sum_{n\geq 0}\frac{a_n x^n}{n!}.$$

Then $g_s(f_r(x)-1)\succcurlyeq g_{r+s}(x)$ *for* $s>0$*, so that*

$$a_n \geq (r+s)^{n-1}$$

for all $n\geq 1$*. Equality holds for* $n=1$ *and* $n=2$ *for all* r,s*; for* $n=3$ *if and only if either* $r=0$ *or* $s=1$*; and for* $n\geq 4$ *if and only if* $r=0$*.*

Proof Our proof splits into three parts. Let

$$F(y)=g_s(f_r(y-1)-1)-1+1/s.$$

We have

$$f_r(y-1)-1=\frac{1}{r+1}(y^{r+1}-1),$$

so

$$F(y)=\frac{1}{s}\exp\left(\frac{s}{r+1}\left(y^{r+1}-1\right)\right).$$

Since $F(y)$ differs from $g_s(f_r(y-1)-1)$ only in the constant term, we have

$$F(y)=-(1-1/s)+\sum_{n\geq 1}\frac{a_n(y-1)^n}{n!},$$

with the a_n as defined in the statement of the theorem. For $n\geq 1$, we have

$$a_n=\frac{\mathrm{d}^n}{\mathrm{d}y^n}\left(F(y)\right)|_{y=1}\ .$$

Let

$$b_n=\frac{\mathrm{d}^n}{\mathrm{d}y^n}\left(F(y)\right).$$

We first claim that, for $n\geq 1$,

$$b_n=sF(y)y^{r+1-n}\sum_{m=0}^{n-1}g_{n,m}(r)s^m y^{(r+1)m}$$

for some polynomial $g_{n,m}(r)$ of degree $n-1-m$ in r. This is clearly true for $n=1$ as $b_1=F'(y)=sy^rF(y)$; for $n=2$ we have $b_2=sy^{r-1}(sy^{r+1}+r)F(y)$. Thus, $g_{1,0}=1$, $g_{2,0}=r$ and $g_{2,1}=1$.

If we assume that the equation holds for some $n = k$, with $k \geq 1$, we have that

$$\begin{aligned}
b_{k+1} &= \frac{\mathrm{d}}{\mathrm{d}y}(b_k) \\
&= s^2 y^r F(y) y^{r+1-k} \sum_{m=0}^{k-1} g_{k,m}(r) s^m y^{(r+1)m} \\
&\quad + (r+1-k) s F(y) y^{r-k} \sum_{m=0}^{k-1} g_{k,m}(r) s^m y^{(r+1)m} \\
&\quad + s F(y) y^{r+1-k} \sum_{m=0}^{k-1} g_{k,m}(r) s^m (r+1) m y^{(r+1)m-1} \\
&= s F(y) y^{r-k} \left(\left(s y^{r+1} + r + 1 - k \right) \sum_{m=0}^{k-1} g_{k,m}(r) s^m y^{(r+1)m} \right. \\
&\quad \left. + \sum_{m=0}^{k-1} (r+1) m g_{k,m}(r) s^m y^{(r+1)m} \right).
\end{aligned}$$

This is of the form required, and so the claim holds for $n = k+1$. Indeed we have

$$g_{k+1,m} = g_{k,m-1} + ((r+1)(m+1) - k) g_{k,m},$$

where the first term is absent if $m = 0$.

Let $S = sy^{r+1}$. Then we see that, for $n \geq 2$,

$$\begin{aligned}
& (S+r+1-n)(S+r)^{n-1} + (n-1)S(r+1)(S+r)^{n-2} \\
= \;& (S+r)^{n-2}\left((S+r+1-n)(S+r) + (n-1)S(r+1)\right) \\
= \;& (S+r)^{n-2}\left((S+r)^2 + (n-1)(S-1)r\right) \\
= \;& (S+r)^n + (n-1)(S+r)^{n-2}(S-1)r.
\end{aligned}$$

We now claim that

$$\begin{aligned}
\frac{b_n}{Sy^{-n}F(y)} &= (S+r)^{n-1} + (n-2)(S-1)r(S+r)^{n-3} \\
&+ \sum_{i,j,l,k \geq 0} \alpha(n,i,j,k,l,\mu) S^i (S-1)^j (r+1)^k r^l \prod_{p=1}^{n-1} (S+r+1-p)^{\mu_p},
\end{aligned}$$

where $\mu = (\mu_1, \ldots, \mu_{n-1})$, $\mu_i \geq 0$ and $\alpha(n, i, j, k, l, \mu) \geq 0$ and $i + j + k + l + \sum \mu_p \leq n - 1$. (The second term is present only if $n \geq 3$.)

Now $b_1/(Sy^{-1}F(y)) = 1$, so the claim holds for $n = 1$ (with the second term absent and the third term containing a single summand with $i = j = k = l = \mu_p = 0$). Similarly, $b_2/(Sy^{-2}F(y)) = S + r$, so the claim holds for $n = 2$. Assume that the claim holds for some $n = k$, with $k \geq 1$. Then

$$\begin{aligned}
& \frac{b_{k+1}}{Sy^{-k-1}F(y)} \\
= \; & (-k + (r+1) + S)\frac{b_k}{Sy^{-k}F(y)} \\
& +(k-1)S(S+r)^{k-2}(r+1) + (k-2)(k-3)(S-1)S(S+r)^{k-4}(r+1)r \\
& +(k-2)S(S+r)^{k-3}(r+1)r \\
& + \sum_{i,j \geq 0} \alpha(n, i, j, k, l, \mu)(r+1)S^{i-1}(S-1)^j(r+1)^k r^l \prod_{p=1}^{n-1}(S+r+1-p)^{\mu_p} \\
& + \sum_{i,j \geq 0} \alpha(n, i, j, k, l, \mu)S^i(r+1)j(S-1)^{j-1}(r+1)^k r^l \prod_{p=1}^{n-1}(S+r+1-p)^{\mu_p} \\
& + \sum_{i,j \geq 0} \alpha(n, i, j, k, l, \mu)S^i(S-1)^j(r+1)^k r^l \times \\
& \quad \times \left(S(r+1) \sum_{\substack{q=1,2,\ldots,n-1 \\ \mu_q \geq 1}} \frac{\mu_q}{(S+r+1-q)} \prod_{p=1}^{n-1}(S+r+1-p)^{\mu_p} \right).
\end{aligned}$$

We split this into two parts. The first part is

$$\begin{aligned}
& (S+r+1-k)(S+r)^{k-1} + (k-1)S(S+r)^{k-2}(r+1) \\
= \; & (S+r)^k + (k-1)(S-1)(S+r)^{k-2}r,
\end{aligned}$$

while the rest has the form

$$\sum_{i,j \geq 0} \alpha(n+1, i, j, k, l, \mu)S^i(S-1)^j(r+1)^k r^l \prod_{p=1}^{n}(S+r+1-p)^{\mu_p}.$$

Finally, we put $y = 1$. We have the required results for $n \leq 3$, so assume that $n \geq 4$ and that $r, s \geq 1$. We have

$$\sum_{i,j \geq 0} \alpha(n, i, j, k, l, \mu)s^i(s-1)^j(r+1)^k r^l \prod_{p=1}^{n-1}(s+r+1-p)^{\mu_p} \geq 0.$$

Now $sy^{-n}F(y)\mid_{y=1}=1$, $S\mid_{y=1}=s$, and so

$$\begin{aligned} a_n &= b_n \mid_{y=1} \\ &\geq (s+r)^{n-1} + (n-2)r(s-1)(s+r)^{n-3} \\ &\geq (s+r)^{n-1}, \end{aligned}$$

with strict inequality if $n > 2$ and $s > 1$.

If $s = 1$ and $n \geq 4$, then the second part of the expression contains a term $(k-2)S(S+r)^{k-3}(r+1)r$. On putting $n = k+1$ and $y = 1$ this becomes $(n-3)s(s+r)^{n-4}(r+1)r$, which is strictly positive; so we have strict inequality. □

4 Recognising imprimitive groups

Lemma 4.1 *Let G be transitive on the infinite set Ω, and suppose that the point stabiliser G_α has s orbits (all infinite) on $\Omega \setminus \{\alpha\}$, and s^2 orbits on ordered pairs of distinct elements from this set. Then G has s infinite blocks of imprimitivity (and so is imprimitive if $s > 1$); it permutes the set of blocks regularly, and the stabiliser of a block acts 3-transitively on it.*

Proof Our proof is by induction on s. It is clear that for $s = 1$, the hypotheses assert that G is 3-transitive. Suppose that $s \geq 2$, and that the lemma holds for values less than s. The hypothesis implies that an orbit of G_α on pairs of distinct points is uniquely determined by the G_α-orbits containing the two points.

First, we claim that G is imprimitive. For let $\{\alpha\}, O_1, \ldots, O_s$ be the orbits of G_α, and choose a point $\beta \in O_1$. Then the orbits of $G_{\alpha\beta}$ are $\{\alpha\}$, $\{\beta\}$, $O_1 \setminus \{\beta\}$, $O_2, \ldots, O_s$. The G_β-orbits are the same except for taking the union of $\{\alpha\}$ with one of the other orbits.

If $s > 2$, at least one orbit O_i is fixed by both G_α and G_β. Since it is not fixed by G, we see that $\langle G_\alpha, G_\beta \rangle$ is a proper subgroup of G, whence G is imprimitive.

For $s = 2$, the same argument applies unless $O_2 \cup \{\alpha\}$ is an orbit of G_β. In this case we see that $\{\alpha\} \cup O_2$ and $\{\beta\} \cup O_1$ are the blocks of imprimitivity.

Choose B to be a minimal block of imprimitivity containing α. Without loss of generality, suppose that $B = \{\alpha\} \cup O_1 \cup \cdots \cup O_t$, for some t with $1 \leq t < s$. Let H be the setwise stabiliser of B, acting on B. Clearly all

H_α-orbits are infinite, and $F_1(H_\alpha) = t$ and $F_2(H_\alpha) = t^2$. The same argument as before shows that, if $t > 1$, then H is imprimitive, contrary to our choice of B as a minimal block. So $t = 1$ and H is 3-transitive on B.

If $i > 1$ and $\beta \in O_1$, then G_α is transitive on $O_1 \times O_i$, so $G_{\alpha\beta}$ is transitive on O_i. Thus, O_i is an orbit of $\langle G_\alpha, G_\beta \rangle = G_B$. It follows that, for $\gamma \in O_i$, the orbits of G_γ are B, $O_i \setminus \{\gamma\}$, and O_j for $j \neq 1, i$. Thus, $O_1, \ldots, O_2$ are the translates of B, and G permutes the blocks $B = O_1 \cup \{\alpha\}$, $O_2, \ldots, O_s$ regularly. □

Now suppose that G has s infinite blocks of imprimitivity and permutes the blocks regularly. Then $F_k(G) = F_{k-1}(G_\alpha) \geq s^{k-1}$, since G_α fixes all s blocks. Equality implies, in particular, that G_α acts $(k-1)$-transitively on the remaining points of the block containing α. So the Theorem is proved.

References

[1] Cameron, P. J. (1990) *Oligomorphic Permutation Groups*, London Math. Soc Lecture Notes 152, Cambridge University Press: Cambridge.

[2] Joyal, A. (1981) Une theorie combinatoire des séries formelles, *Advances in Math.* 42: 1–82.

[3] Macpherson, H. D. (1983) The action of an infinite permutation group on the unordered subsets of a set, *Proc. London Math. Soc.* (3) 46: 471–486.

[4] Merola, F. (2001) Orbits on n-tuples for infinite permutation groups, *Europ. J. Combinatorics* 22: 225–241.